AMENDMENTS TO THE DRAWINGS

The attached one sheet of drawing includes the following change:

In Fig. 2, the label "PRIOR ART" has been added.

Attachment: 1 Replacement Sheet

REMARKS

Claims 1-27 are pending in the application. In response to the Office Action mailed October 18, 2005, it is respectfully submitted that pending claims 1-27 define patentable subject matter.

Applicant is filing concurrently herewith a Petition for a Three-Month Extension of Time, thereby extending the time for responding to the outstanding Office Action to April 18, 2005.

In the Office Action, Fig. 2 was objected to because it was not labeled as "PRIOR ART". Applicant is herein submitting a proposed drawing correction for Fig. 2. The Examiner is respectfully requested to approve this proposed drawing correction for Fig. 2.

Claim 4 was objected to because of an informality. By this Amendment, Applicant has herein corrected the informality in claim 4. The Examiner is respectfully requested to withdraw this objection of record.

Claims 1-3, 5-8, 10-13, 15-19, 21-23 and 25-27 were rejected under 35 U.S.C. § 102 as being anticipated by Yavatkar et al (U.S. Patent No. 6,735,702). Claim 24 was rejected under 35 U.S.C. § 103 as being unpatentable over Yavatkar et al. Claims 4, 9, 14 and 20 were rejected under 35 U.S.C. § 103 as being unpatentable over Yavatkar in view of Cox et al (U.S. Patent No. 6,738,814). Applicant respectfully traverses these 35 U.S.C. § 102 and 103 rejections for the following reasons.

The claimed invention relates to a method and apparatus for preventing bandwidth congestion on a network. According to claim 1, in response to the detection of an overload condition, the method automatically blocks the origination client or clients responsible for the

overload condition form accessing the Internet through its or their respective connection points. The remaining independent claims 5, 10, 12, 15, 16, 17 and 18 specify that the method or apparatus identifies the attacking address corresponding to the attacking site from which the bandwidth congestion originated and prevents the attacking address corresponding to the attacking site from being used to gain access to the Internet or other WAN.

It is respectfully submitted that Yavatkar et al does not describe or suggest the features in the pending independent claims.

Yavatkar et al relates to a system for analyzing traffic on a network by monitoring network traffic, and when an attack is detected, gathering information about the traffic on the network by launching a watchdog agent that iteratively follows the attack traffic in an attempt to move closer to the source of the attack traffic (see the flowchart shown in Fig. 9 of Yavatkar et al). In step 426, the watchdog agent 114 may report or respond to the attack. For example, watchdog agent 114 may alter routing tables to prohibit attack traffic or may create an agent which acts as a firewall to prevent such traffic from entering the network. Alternatively, the watchdog agent 114 may report findings to a network administrator who may attempt to cure the problem. (Col. 21, lines 29-36).

In rejecting claim 1 as being anticipated by Yavatkar et al, the Examiner indicates that col. 17, lines 20-27 of Yavatkar et al describes the feature of blocking the origination client from accessing the Internet through its connection point(s) (see the first full paragraph on page 3 of the Office Action). However, it is respectfully submitted that Yavatkar et al does not disclose or suggest this feature found in claim 1.

Claim 1 specifically recites that "blocking the origination client(s)" from access to the Internet. Yavatkar et al fails to disclose or suggest blocking the origination client, let alone blocking the origination client from accessing the Internet. Rather, in Yavatkar et al, the system performs an iterative procedure, ending at a node at which attack traffic enters the network. In fact, Yavatkar et al specifically teaches that this node is not the originating source, but rather just the source of the attack traffic to the network:.

> Such a node may be considered to be the source of the attacking traffic-while ***it is not the originating source***, it is the source of the attack traffic to the network. (Col. 17, lines 22-24; emphasis added).

As is apparent, the Yavatkar et al system fails to teach "blocking the origination client or clients", as required in claim 1. Rather, Yavatkar et al teaches blocking a node to the network where the attack traffic first enters. Since Yavatkar et al fails to teach each and every feature in claim 1, Yavatkar et al cannot anticipate this claim. Moreover, there is no suggestion in Yavatkar et al of identifying the origination client. Rather, Yavatkar et al teaches a different method of stopping attack traffic, by identifying the node at which attack traffic first enters the network. Since Yavatkar et al fails to suggest the feature of identifying an origination client that is responsible for the overload condition, Yavatkar et al fails to suggest the method of claim 1.

It should be noted that with the Yavatkar et al system, all traffic from the identified node is block, even traffic that originates from a client that is not responsible for the overload condition. In contrast, in the method defined in claim 1, the origination client is identified and the origination client is blocked from accessing the Internet through its connection point. Other clients that are not responsive for the overload condition could still access the Internet. This

claimed method is highly desirable relative to the scheme described in Yavatkar et al which blocks all traffic, even traffic that is not causing an overload condition.

The remaining independent claims 5, 10, 12, 15, 16, 17 and 18 all recite the feature of identifying an address corresponding to the attacking site from which bandwidth congestion originated, and then preventing that attacking address from being able to access the Internet. Yavatkar et al fails to describe or suggest identifying such an address, let alone blocking the attacking address. Rather, as described above, Yavatkar et al goes about preventing bandwidth congestion in a completely different way. In Yavatkar et al, the system iteratively determines the offending node and then blocks all traffic at that node. There is no suggestion of identifying an attacking address and then blocking the identified attacking address from accessing the Internet. Consequently, it is respectfully submitted that the remaining independent claims define patentable subject matter relative to Yavatkar et al.

The teachings of Cox do not remedy the deficiencies of Yavatkar et al. It is respectfully submitted that the teachings of Cox in combination of Yavatkar et al fails to teach or suggest the claimed invention. Referring to page 14 of the Office Action, the Examiner cites Cox for its teaching in col. 4, line 62 through col. 5, line 3. However, these cited portions of Cox teach a method for preventing address spoofing. That is, Cox teaches a cache of internal addresses and compares an address corresponding to an external request with the cache list to determine whether or not address spoofing is occurring. Cox fails to teach identifying an attacking client's address corresponding to an overload condition, and then blocking that client address from connecting to the Internet. Rather, in Cox, the external request is permitted to propagate through the Internet until it reaches the network with the cache containing the list of addresses. If the

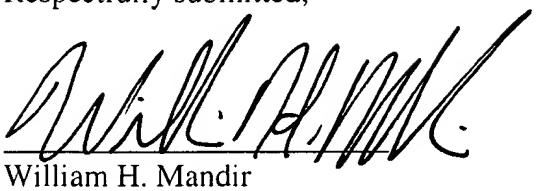
address is found on the cache list, then the request packet is discarded (Col. 4, line 67 to col. 5, line 1). In contrast, according to the claimed invention, the address of the origination client is identified and forwarded to the origination router for the original client so that the origination client is prevented from being able to connect to the Internet. Cox fails to disclose or suggest this claimed feature. In Cox, the address of the external request is compared after it is received by network; Cox fails to identify the address to the original client's router to prevent access at that point.

As is apparent, there are substantial structural and functional differences between the claimed invention and the cited prior art references. None of the prior art references teaches or suggests identifying an origination client, by for example, identifying the address of the original client, and then using this address to prevent the original client from accessing the origination client's router.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



William H. Mandir
Registration No. 32,156

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: April 18, 2005